UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/386,341	08/31/1999	RYU INADA	104116	1319

25944 7590 02/03/2004

OLIFF & BERRIDGE, PLC
P.O. BOX 19928
ALEXANDRIA, VA 22320

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	**PAPER NUMBER**
2132	11

DATE MAILED: 02/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/386,341	INADA, RYU	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6 and 8-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *9-13 and 19* is/are allowed.

6)☒ Claim(s) *1-6 and 14-18* is/are rejected.

7)☒ Claim(s) *8* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

Response to Arguments

1. This communication is in response to applicant's response received on November 21, 2003.

2. The terminal disclaimer filed on November 21, 2003 by the applicant, is accepted and the examiner withdraws the double patenting rejections.

3. The amendments to claims 1, 3-6, 9-10 and 15 and cancellation of claim 7 are acknowledged and that these amendments do not introduce any new matter to the claimed invention.

4. On page 3 of the amendment, it is indicated that claim 2 has been amended, but this claim is still original and has not been amended.

5. On page 7 of the amendment, it is indicated that claim 14 is the original claim, but this claim has been amended.

6. On page 11 of the amendment, "Regarding claim 4", applicant states that the word "a" has been inserted between the words "acquiring" and "signature", but on page 4 of the amendment this insertion has not been implemented.

7. Applicants' arguments have been fully considered but they are not persuasive.

Specification

The substitute specification filed November 21, 2003 has not been entered because it does not conform to 37 CFR 1.125(b) and (c) because: the substitute specification has not been written in a clear and comprehensible fashion and it is inconsistent in some parts. See the following examples:

1. Claim 6, lines 5 and 6, states that "...a desire function including an inverse function..." but according to the paragraph [0018] of the specification which states "...private key is modified by use of a function which is not a one-directional function (including an inverse function)..." the inverse function is not included in a desire function, which is inconsistent with the claim 6.

2. The recited term "encryption target data" in claim 1 and other claims has not been clearly described in the substitute specification. There is also no clear distinction among the "encryption target data", paragraph [0009], line 6, "signature target data", paragraph [0014], line 10, "encryption target", paragraph [0019], line 7, "target range", paragraph [0100], line 8, "target data", paragraph [0100], line 13, "judgment target", paragraph [0138], line 2 and "signature target", paragraph [0156], line 2. These

terminologies have been used interchangeably throughout the specification without sufficient descriptions.

3. The last sentences of paragraphs [0003], [0004], the last two sentences of paragraph [0005] and paragraph [0007], for examples, are not comprehensible. This pattern seems to be prevalent throughout the specification.

4. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

5. A substitute specification in proper idiomatic English and in compliance with 37 CFR 1.52(a) and (b) is required. The substitute specification filed must be accompanied by a statement that it contains no new matter.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 3, 16 and 17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 3, lines 7 and 8, the statement "... used to generate said common key" is unclear. Appropriate correction as has been applied to claim 4, line 8, is necessary.

Regarding claim 16, line 3, the statement "... by encrypting a private key corresponding to said common key by use of a common key..." is unclear. Appropriate correction is necessary.

Regarding claim 16, line 7, contains "lock data". There is insufficient antecedent basis for this in the claim.

Regarding claim 17, line 3, the statement "... by encrypting a private key corresponding to said common key by use of a common key..." is unclear. Appropriate correction is necessary.

Regarding claim 17, line 7, contains "lock data". There is insufficient antecedent basis for this in the claim.

Claim Rejections - 35 USC § 102

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-6, 14-16 and 18 are rejected under 35 U.S.C. 102(e) as being anticipated by Okamoto et al (6,118,874) (hereinafter referred to as Okamoto).

Referring to claims 1, 3, 5, 14-16 and 18, Okamoto discloses a method and system for encrypted data and key recovery (see abstract and Figs. 6A and 6B). Okamoto discloses generating an enveloped data (corresponding to the recited lock data) by combining an encrypted plaintext m (corresponding to the recited a private key) generated by using of a common key and encrypted said common key(s) generated by using the public keys of the members of a group (see, for example col. 1, line 59-col. 2, line 26 and col. 7, lines 3-13). Okamoto further discloses that the encrypted common key (data key) is decrypted by the user's private key (see, for example col. 2, line 6-8,

col. 7, lines 19-25, and col. 10, lines 1-10) and the decrypted common key is used to decrypt the encrypted cipher text (see, for example col. 2, line 8-11).

Okamoto also discloses that the public key and the private key of each key storage apparatus are used to encrypt and decrypt the split secret key (corresponding to the recited encryption target data) of a user (see, for example, col. 5, line 50-53, col. 6, lines 10-15, col. 12, lines 8-11 and col. 13, lines 27-28).

Referring to claim 2, Okamoto discloses that the split secret key (corresponding to the recited encryption target data) is a user's private key which is used for decryption (see, for example, col. 10, lines 1-4)

Referring to claims 4 and 17, this claim is rejected as applied to the like elements of claims 1 and 2 as stated above and further the following:

Okamoto discloses the use of public key certificate (corresponding to the recited writing a signature on the target data) to verify the user private key (see, for example, col. 4, line 65-67, col. 7, lines 50-54 and col. 10, lines 35-40).

Referring to claim 6, this claim is rejected as applied to the like elements of claims 1 and 2 as stated above and further the following:

Okamoto discloses that the private key is split in pieces (corresponding to the recited modifying the private key by use of a desired function) before being encrypted (see, for example, col. 2, lines 58-67 and col. 9, lines 55-60).

Allowable Subject Matter

1. Claim 8 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

2. Claims 9-13 and 19 are allowed.

3. The following is an examiner's statement of reasons for allowance:

4. The primary reasons for the allowance of the independent claims 9 and 19 are the inclusion of the following limitations that are not found in the prior art and they are uniquely distinct features. The closest prior art is Okamoto et al (6,118,874). Okamoto discloses a system and method for encrypted key and data recovery. Okamoto method encrypts the split pieces of private keys by using a common data key. The public keys of key storage apparatuses are used to encrypt the common data key. Okamoto discloses the generation of an enveloped data, which includes the encrypted private key and the encrypted common key. However, Okamoto art fails to anticipate or render the following limitations:

"Claim 9: storing lock data including a first public key, an encrypted private key formed by encrypting a private key corresponding to said first public key by use of a common key, a plurality of encrypted common keys formed by encrypting said common key by use of public keys of respective group/members, a second public key for verifying a signature, an encrypted signature private key formed by encrypting a signature private key for writing said signature by use of a public key of a changing right holder, said first public key, said encrypted private key, said encrypted common key, said second public key, and a signature written by use of said signature private key on said encrypted signature private key; and

decrypting said encrypted signature private key included in said lock data by use of said private key of a changing right holder."

"Claim 19: a memory part that stores lock data including a first public key, an encrypted private key formed by encrypting a private key corresponding to said first public key by use of a common key, a plurality of encrypted common keys formed by encrypting said common key by use of public keys of respective group/members, a second public key for verifying a signature, an encrypted signature private key formed by encrypting a signature private key for writing said signature by use of a public key of a changing right holder, said first public key, said encrypted private key, said encrypted common key, said second public key, and a signature written by use of said signature private key on said encrypted signature private key; and

a generating part that decrypts said encrypted signature private key included in said lock data by use of said private key of a changing right holder to generate a signature private key."

5. The dependent claims 10-13 are allowed because they were originally found to include a unique feature not found in the closest abovementioned art.

6. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 703-305-8074. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-746-7239.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Abdulhakim Nobahar
Examiner
Art Unit 2132

AN
January 27, 2004

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100